Fig. 1

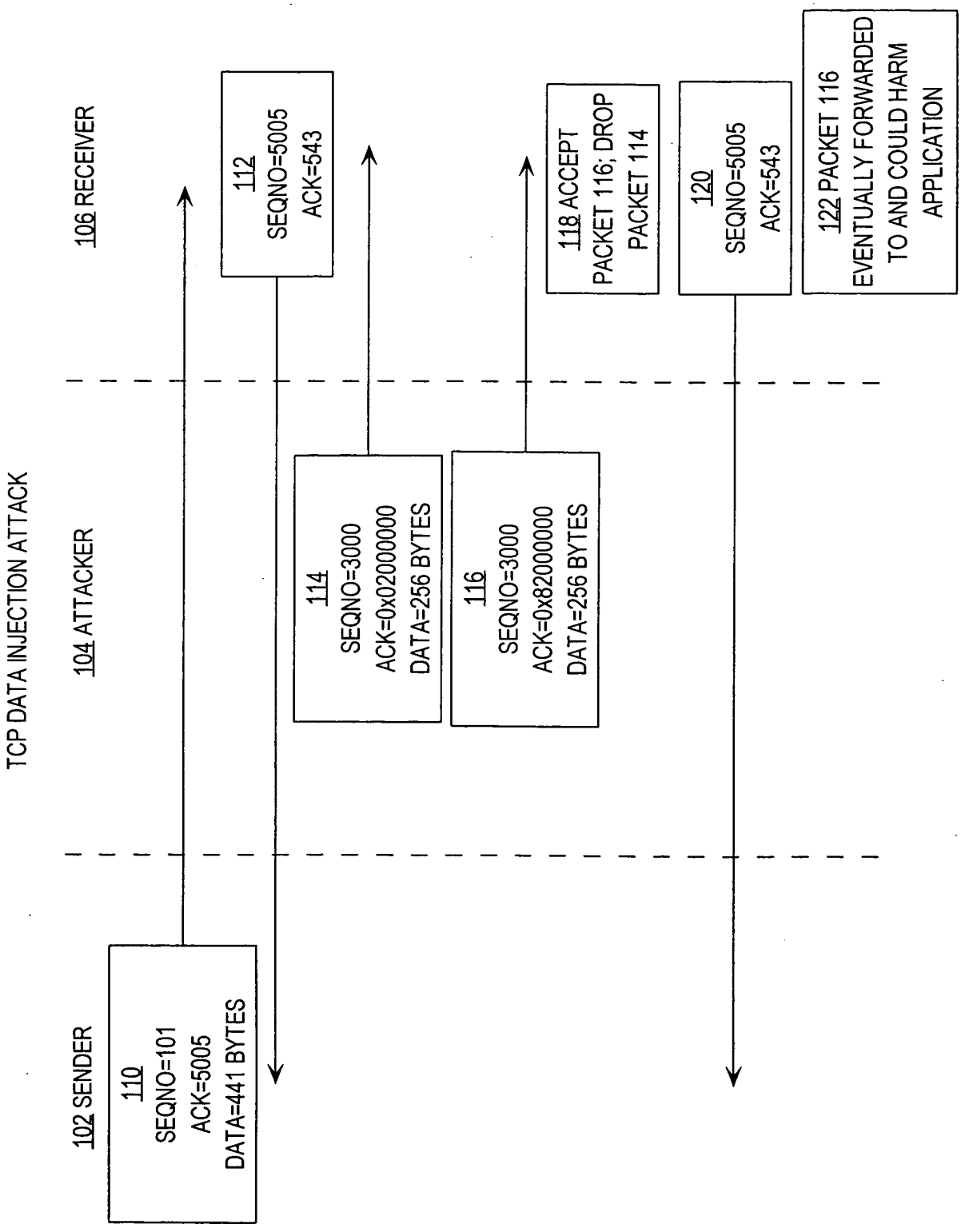

TCP DATA INJECTION ATTACK
102 SENDER
104 ATTACKER
106 RECEIVER
110 SEQNO=101 ACK=5005 DATA=441 BYTES
112 SEQNO=5005 ACK=543
114 SEQNO=3000 ACK=0x02000000 DATA=256 BYTES
116 SEQNO=3000 ACK=0x82000000 DATA=256 BYTES
118 ACCEPT PACKET 116; DROP PACKET 114
120 SEQNO=5005 ACK=543
122 PACKET 116 EVENTUALLY FORWARDED TO AND COULD HARM APPLICATION

Fig. 2

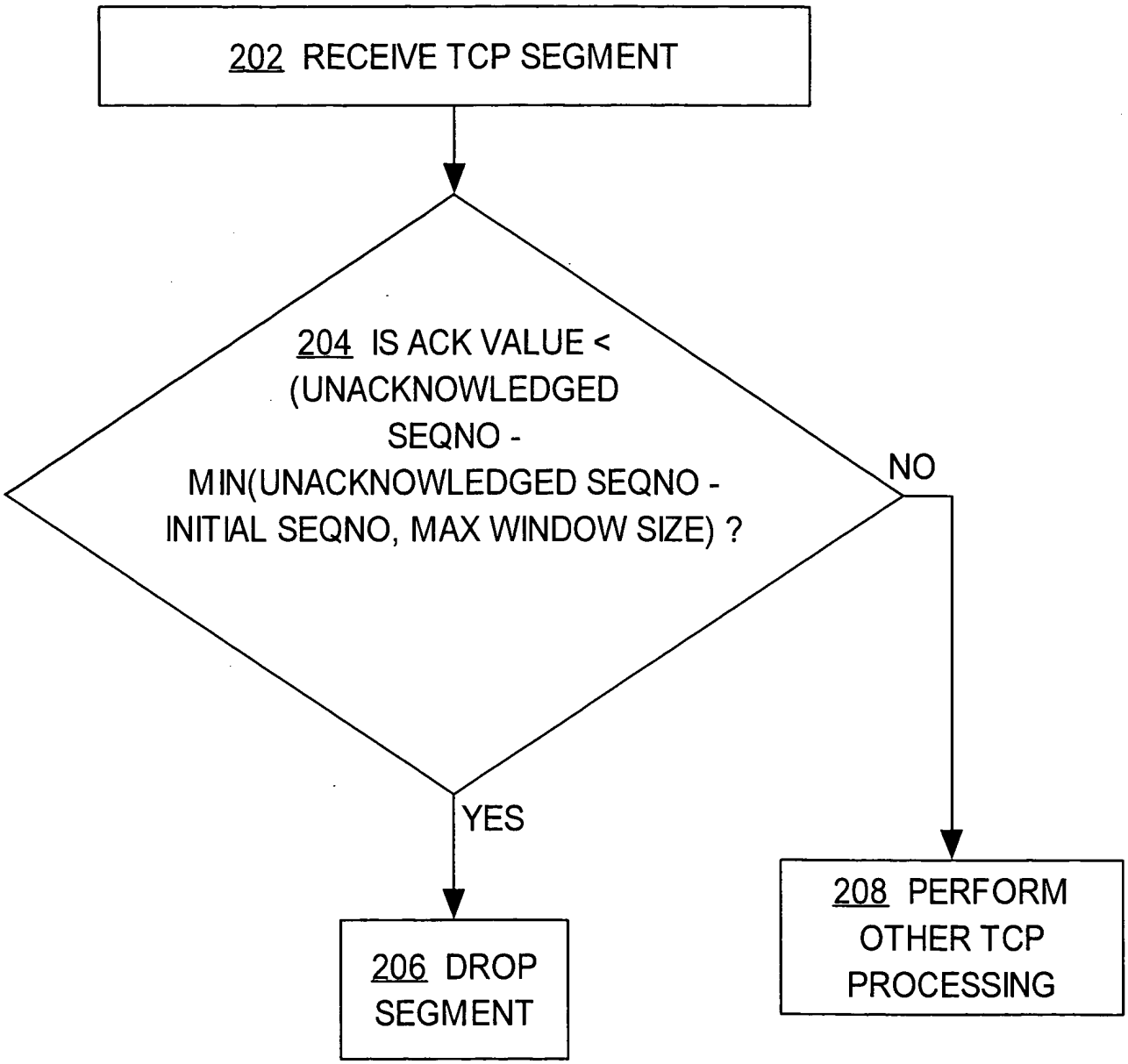

202 RECEIVE TCP SEGMENT
204 IS ACK VALUE < (UNACKNOWLEDGED SEQNO - MIN(UNACKNOWLEDGED SEQNO - INITIAL SEQNO, MAX WINDOW SIZE) ?
NO
YES
206 DROP SEGMENT
208 PERFORM OTHER TCP PROCESSING

Fig. 4

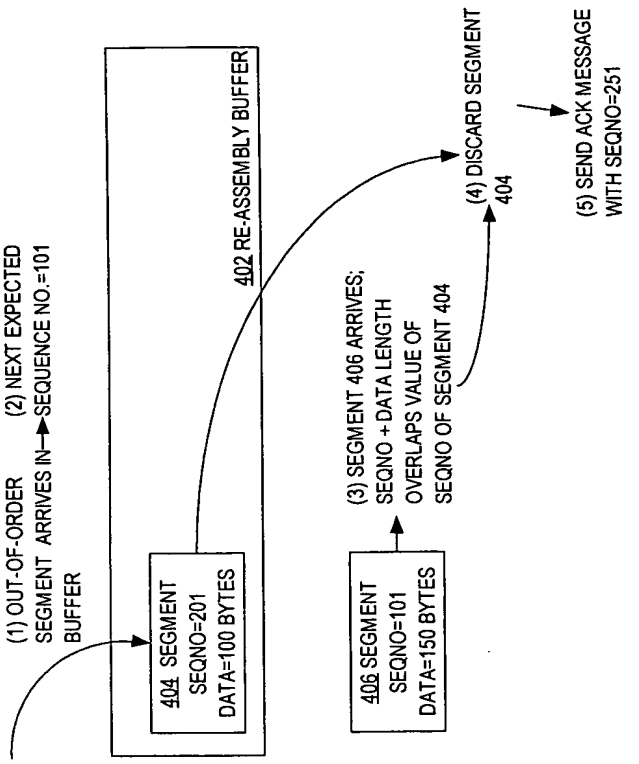

(1) OUT-OF-ORDER SEGMENT ARRIVES IN BUFFER
(2) NEXT EXPECTED SEQUENCE NO.=101
402 RE-ASSEMBLY BUFFER
404 SEGMENT SEQNO=201 DATA=100 BYTES
406 SEGMENT SEQNO=101 DATA=150 BYTES
(3) SEGMENT 406 ARRIVES; SEQNO + DATA LENGTH OVERLAPS VALUE OF SEQNO OF SEGMENT 404
(4) DISCARD SEGMENT 404
(5) SEND ACK MESSAGE WITH SEQNO=251

Fig. 3

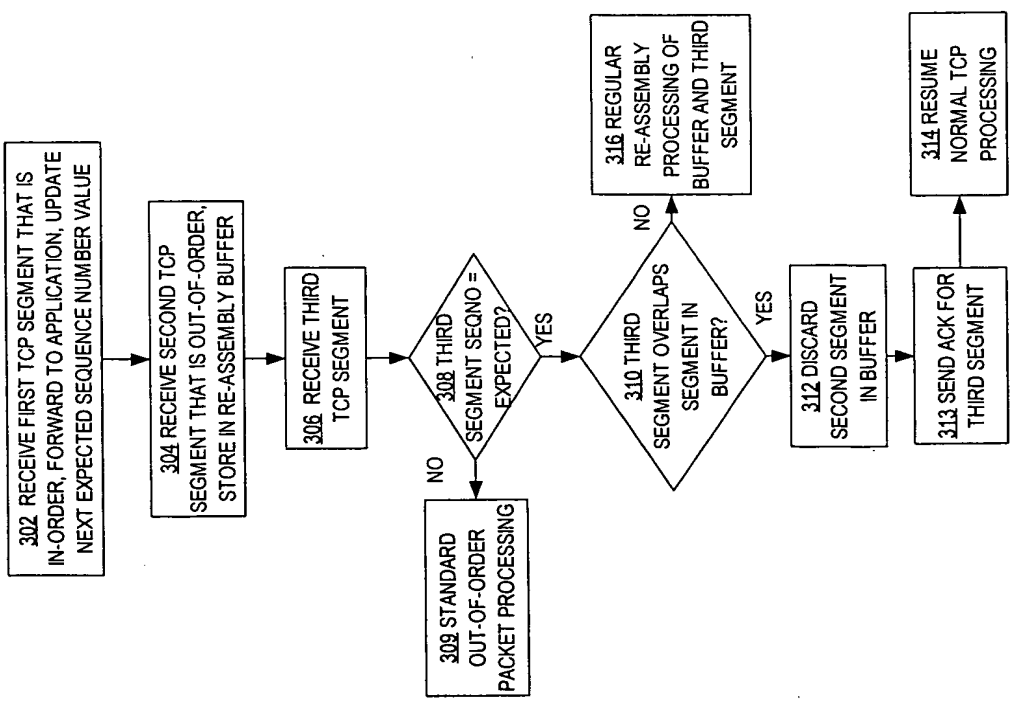

302 RECEIVE FIRST TCP SEGMENT THAT IS IN-ORDER, FORWARD TO APPLICATION, UPDATE NEXT EXPECTED SEQUENCE NUMBER VALUE
304 RECEIVE SECOND TCP SEGMENT THAT IS OUT-OF-ORDER, STORE IN RE-ASSEMBLY BUFFER
306 RECEIVE THIRD TCP SEGMENT
308 THIRD SEGMENT SEQNO = EXPECTED?
NO
YES
309 STANDARD OUT-OF-ORDER PACKET PROCESSING
310 THIRD SEGMENT OVERLAPS SEGMENT IN BUFFER?
NO
YES
316 REGULAR RE-ASSEMBLY PROCESSING OF BUFFER AND THIRD SEGMENT
312 DISCARD SECOND SEGMENT IN BUFFER
313 SEND ACK FOR THIRD SEGMENT
314 RESUME NORMAL TCP PROCESSING

Fig. 5A

DUPLICATE ACK METHOD--STEPS AS PERFORMED BY SENDER AS ATTACKER IS SENDING SPURIOUS SEGMENTS

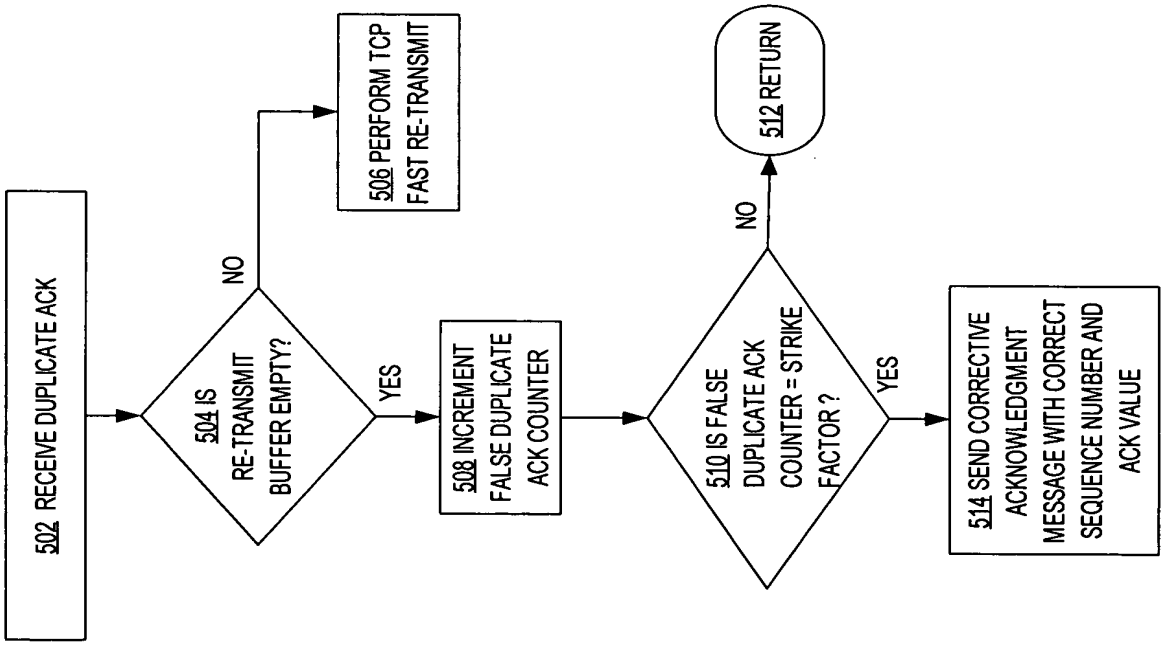


Fig. 5B

DUPLICATE ACK METHOD--RECEIVER'S STEPS

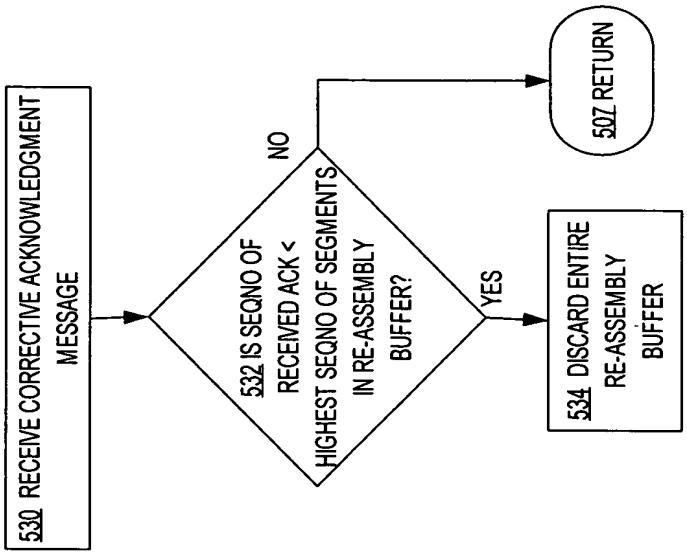
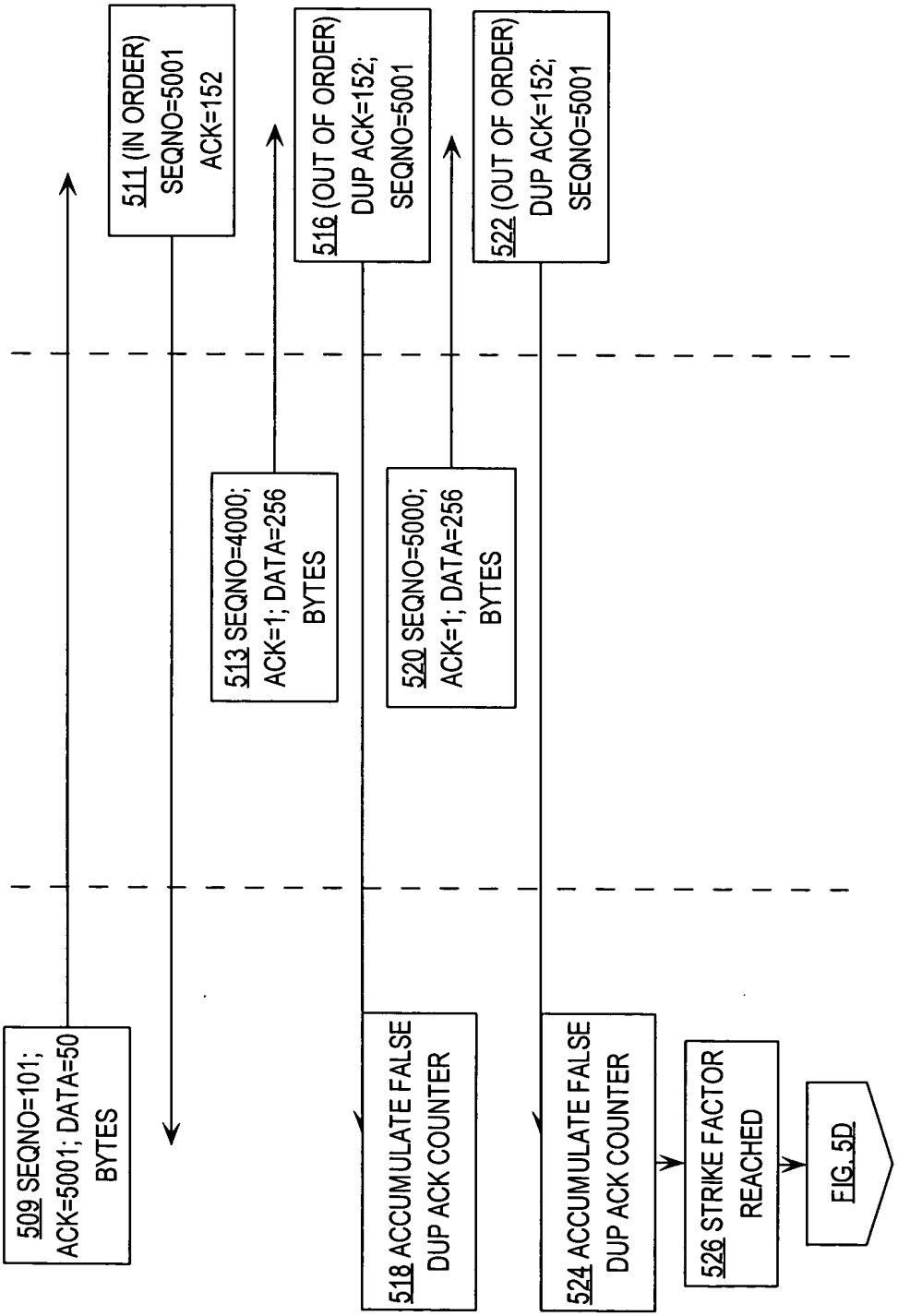


Fig. 5C

TCP DATA INJECTION ATTACK WITH DEFENSE USING DUPLICATE ACK APPROACH



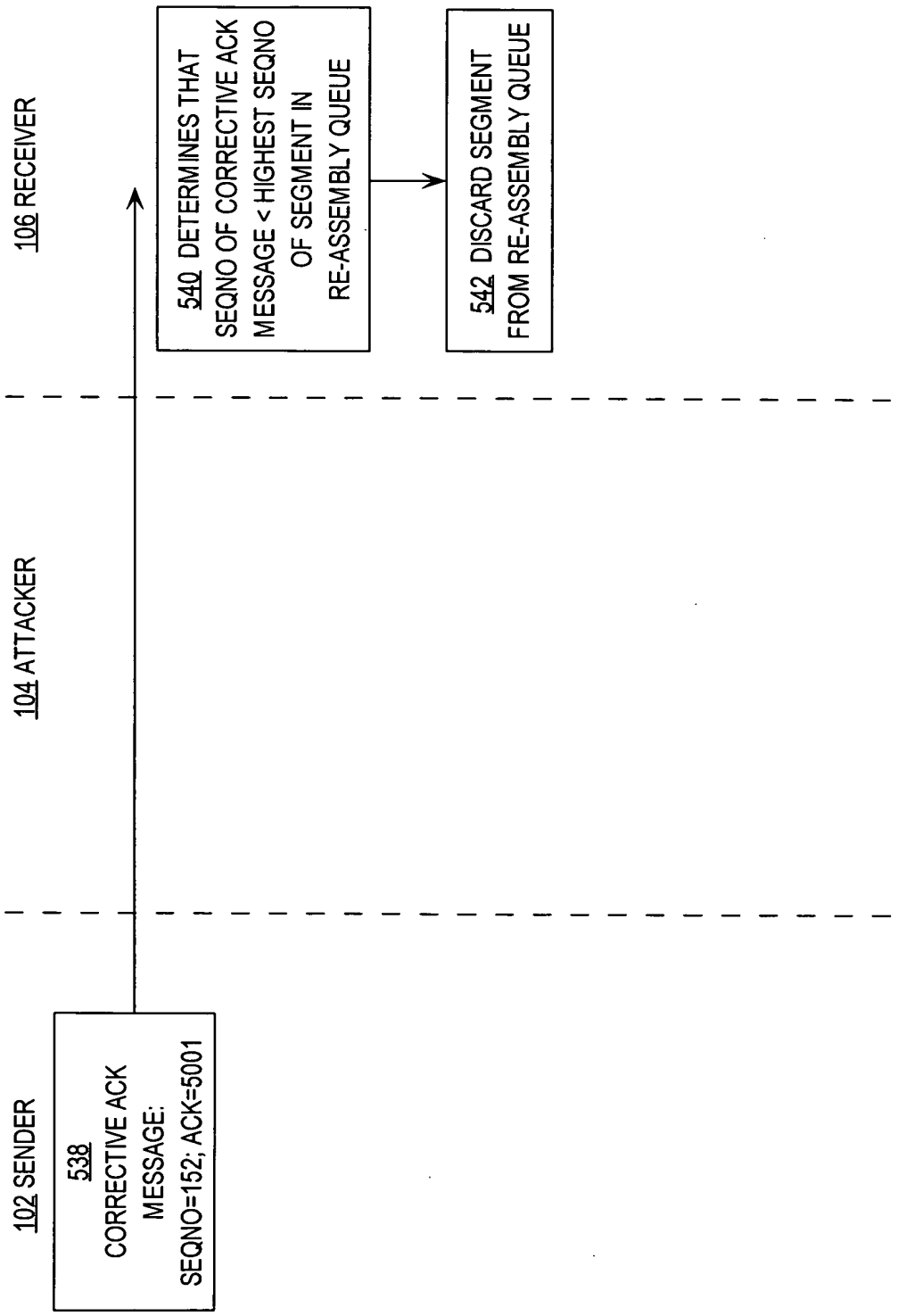
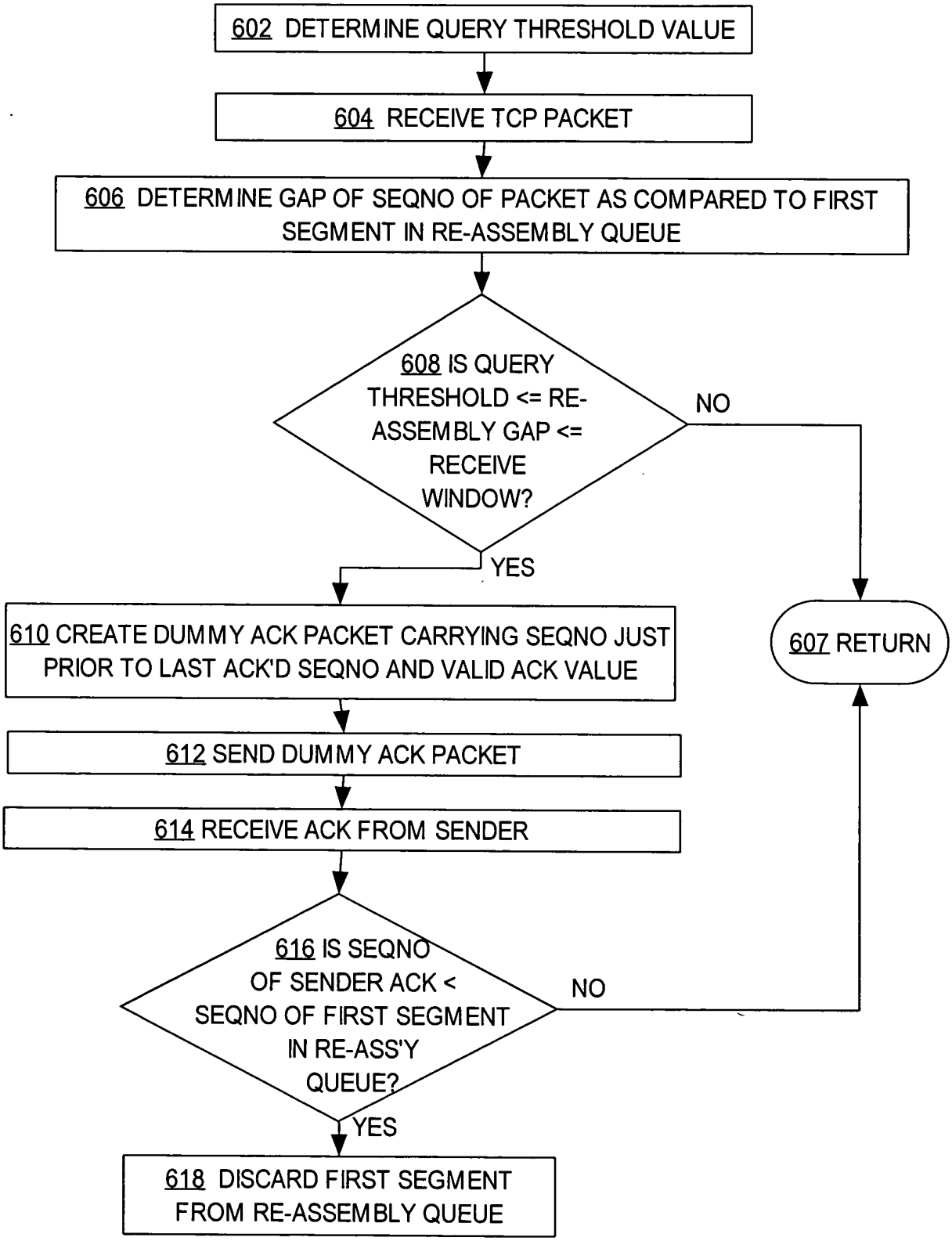

102 SENDER
538
CORRECTIVE ACK
MESSAGE:
SEQNO=152; ACK=5001
104 ATTACKER
106 RECEIVER
540 DETERMINES THAT
SEQNO OF CORRECTIVE ACK
MESSAGE < HIGHEST SEQNO
OF SEGMENT IN
RE-ASSEMBLY QUEUE
542 DISCARD SEGMENT
FROM RE-ASSEMBLY QUEUE

Fig. 5D

Fig. 6


602 DETERMINE QUERY THRESHOLD VALUE
604 RECEIVE TCP PACKET
606 DETERMINE GAP OF SEQNO OF PACKET AS COMPARED TO FIRST SEGMENT IN RE-ASSEMBLY QUEUE
608 IS QUERY THRESHOLD <= RE-ASSEMBLY GAP <= RECEIVE WINDOW?
NO
YES
610 CREATE DUMMY ACK PACKET CARRYING SEQNO JUST PRIOR TO LAST ACK'D SEQNO AND VALID ACK VALUE
607 RETURN
612 SEND DUMMY ACK PACKET
614 RECEIVE ACK FROM SENDER
616 IS SEQNO OF SENDER ACK < SEQNO OF FIRST SEGMENT IN RE-ASS'Y QUEUE?
NO
YES
618 DISCARD FIRST SEGMENT FROM RE-ASSEMBLY QUEUE

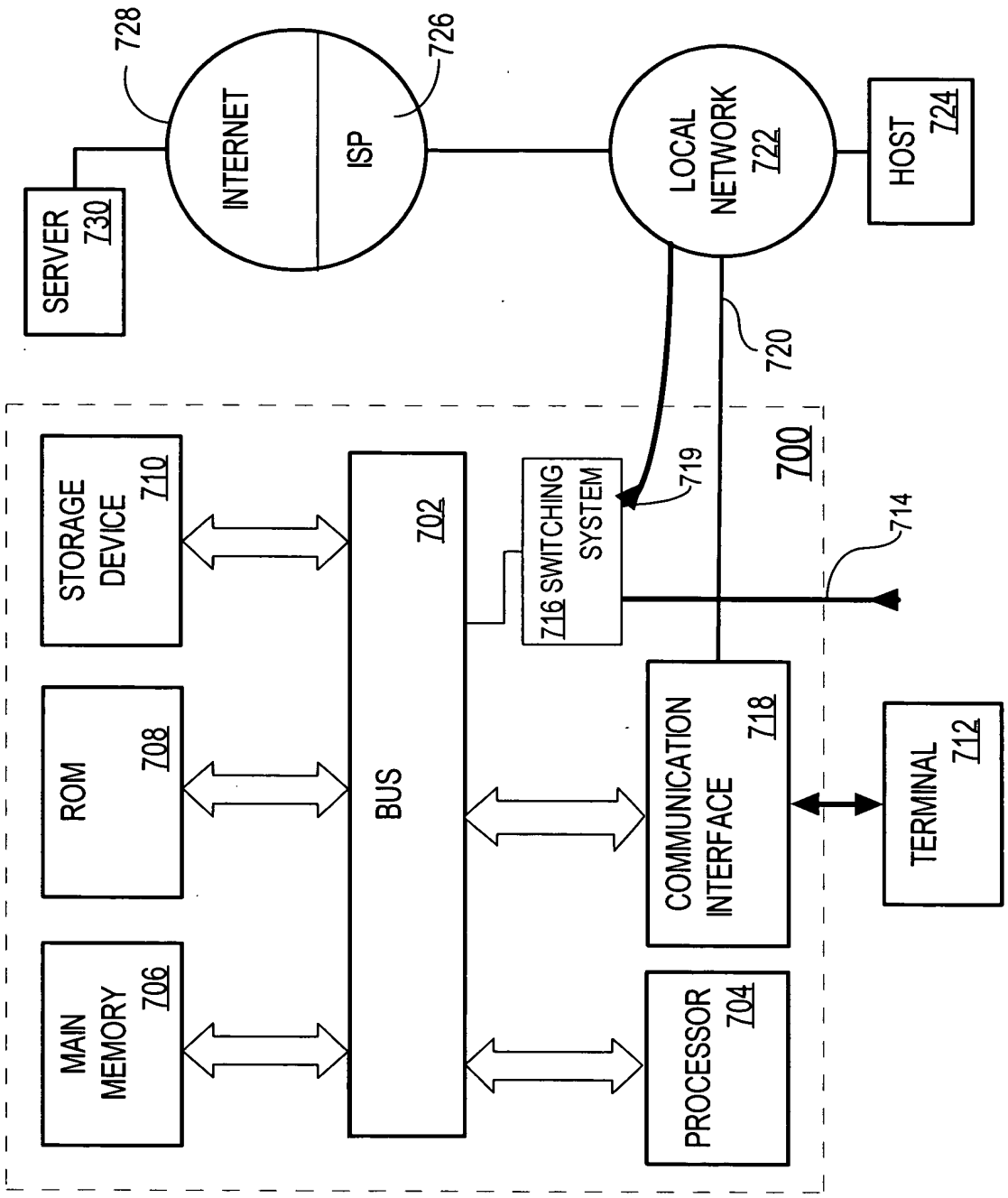

728
INTERNET
ISP
726
SERVER 730
LOCAL NETWORK 722
HOST 724
720
700
719
714
STORAGE DEVICE 710
716 SWITCHING SYSTEM
702
ROM 708
BUS
COMMUNICATION INTERFACE 718
TERMINAL 712
MAIN MEMORY 706
PROCESSOR 704
INPUT DEVICE 714
CURSOR CONTROL 716

FIG. 7